AMENDMENTS TO THE CLAIMS

Applicant submits below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Original) A method for establishing a secure communications channel and authenticating a party, for use by an initiator in an Internet Security Protocol (IPSec) negotiation, comprising:

initiating an Internet Key Exchange (IKE) negotiation with a responder;

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator;

receiving, from the responder, a public DH key of the responder;

transmitting, to the responder, a payload encrypted with a shared secret created from the public DH key of the responder and the private DH key corresponding to the public DH key of the initiator transmitted to the responder;

receiving, from the responder, a payload encrypted with the shared secret; and decrypting the payload;

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator.

2. (Original) The method of claim 1 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

3. (Currently amended) The method of claim 2 wherein the responder comprises a computing device and has previously obtained the public DH key of the initiator from a portable media device, separate from and connectable to the computing device.

4. (Original) The method of claim 1 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

5. (Currently amended) The method of claim 4 wherein the initiator comprises a computing device and has previously obtained the public DH key of the responder from a portable media device, separate from and connectable to the computing device.

6. (Original) The method of claim 1 wherein the secure communications channel is a channel in a virtual private network (VPN).

7. (Original) The method of claim 6 wherein the VPN comprises a client and a server, and a public DH key of the VPN client is transmitted as a hint to the identity of the client.

8. (Original) A method for establishing a secure communications channel and authenticating a party, for use by a responder in an Internet Security Protocol (IPSec) negotiation, comprising:

receiving an Internet Key Exchange (IKE) negotiation request from an initiator;

transmitting, to the initiator, a public Diffie-Hellman (DH) key of the responder;

receiving, from the initiator, a public DH key of the initiator;

transmitting, to the initiator, a payload encrypted with a shared secret created from the public DH key of the initiator and the private DH key corresponding to the public DH key of the responder transmitted to the initiator;

receiving, from the initiator, a payload encrypted with the shared secret; and decrypting the payload;

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator.

9. (Original) The method of claim 8 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

10. (Currently amended) The method of claim 9 wherein the responder comprises a computing device and has previously obtained the public DH key of the initiator from a portable media device, separate from and connectable to the computing device.

11. (Original) The method of claim 8 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

12. (Currently amended) The method of claim 11 wherein the initiator comprises a computing device and has previously obtained the public DH key of the responder from a portable media device, separate from and connectable to the computing device.

13. (Original) The method of claim 8 wherein the secure communications channel is a channel in a virtual private network (VPN).

14. (Original) The method of claim 13 wherein VPN comprises a client and a server, and a public DH key of the VPN client is received as a hint to the identity of the client.

15. (Currently amended) A method of establishing, between an initiator and a responder, a secure communications channel following the Internet Security Protocol (IPSec), comprising using the Internet Key Exchange (IKE) protocol, wherein a static Diffie-Hellman (DH) key-pair is used by at least one of the initiator or the responder to establish confidentiality and authentication whereby decryption of a message encrypted with the static Diffie-Hellman key-pair authenticates a device associated with the static key-pair.

16. (Original) The method of claim 15 wherein the private DH key of the DH key-pair is used to create a claim of identity for the initiator or the responder.

17. (Original) The method of claim 15 wherein the secure communications channel is a channel in a virtual private network.

18. (Currently amended) A system for establishing a secure communications channel between networked devices connected over a network, the system comprising:

a first networked device generating a ~~Diffie-Hellman (DH)~~ key pair, the pair comprising a public key and a private key;

a portable media device storing the public key of the ~~DH~~ key pair generated by the first networked device;

a second networked device receiving the public key of the key pair over the network as part of an exchange of message establishing an IPsec security association and reading the public key of the ~~DH~~ key pair from the portable media device; and

the second networked device using the public key of the DH key pair to ensure confidentiality and authenticity in securing a communications channel with another networked device, following the Internet Key Exchange (IKE) and Internet Security (IPSec) protocols,

wherein the portable media device is separate from the network and from the first and second networked devices and is connectable to the second networked device.

19. (Original) The system of claim 18 wherein the secure communications channel is a channel in a virtual private network.

20. (Original) A computer-readable medium including computer-executable instructions facilitating establishing a secure communications channel and authenticating a party, for execution by an initiator in an Internet Security Protocol (IPSec) negotiation, said computer-executable instructions executing the steps of:

initiating an Internet Key Exchange (IKE) negotiation with a responder;

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator;

receiving, from the responder, a public DH key of the responder;

transmitting, to the responder, a payload encrypted with a shared secret created from the public DH key of the responder and the private DH key corresponding to the public DH key of the initiator transmitted to the responder;

receiving, from the responder, a payload encrypted with the shared secret; and decrypting the payload;

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator.

21. (Original) The computer-readable medium of claim 20 wherein the public DH key of the responder is previously known to the initiator and is as a claim on the identity of the responder.

22. (Original) The computer-readable medium of claim 20 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

23. (Original) The computer-readable medium of claim 20 wherein the secure communications channel is a channel in a virtual private network.